2M

УДК 004.89

Н.А. Маслова
Донецкий национальный технический университет, КП «Компания “Вода Донбасса”»
г. Донецк, Украина
masgpp@list.ru

О применении интеллектуального анализа данных для защиты информации корпоративных систем

В статье предлагается методика построения адаптивной саморазвивающейся системы защиты информации для корпоративных систем. При построении системы использованы методы и базовые подходы интеллектуального анализа данных. Система предназначена для решения единой задачи защиты компьютерных сетей, баз данных и систем автоматической обработки информации. Приведены элементы использования методологии интеллектуального анализа данных в системе водоснабжающей отрасли.

Введение

Интеллектуальный анализ данных (ИАД) является одним из прогрессивных способов анализа больших объемов данных. Это процесс обнаружения и дальнейшего применения знаний или ранее неизвестной информации из уже имеющихся наборов [1], основными задачами которого являются классификация; ассоциация; кластеризация; прогнозирование; последовательность.

Инструментальные средства создания интеллектуальных приложений представлены разработками фирм компании Cognos, средства G2 фирмы Gensym Corp, MineSet фирмы Silicon Graphics, Intelligent Miner фирмы IBM, IDIS фирмы Information Discovery. Универсальные средства ИАД довольно сложны и дороги, поэтому они не всегда применяются в интегрированных системах, ориентированных на конечного пользователя.

Интеллектуальный анализ данных используется во многих сферах деятельности современного общества, помогая решать разнообразнейшие задачи. Это, например, страхование, банковское дело, маркетинг, анализ финансовых рисков, мониторинг оборудования и технологических процессов, телекоммуникации, компьютерная безопасность и т.д.

В области компьютерной безопасности методы ИАД тесно связаны с созданием перспективных систем защиты информации (СЗИ). Именно методология ИАД помогает реализовать в СЗИ эволюционные свойства адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности в виде доступной для анализа системы нечетких правил.

Интеллектуальный анализ в корпоративных информационных системах

Наиболее сложными современными информационными структурами, ориентированными на крупные компании, являются корпоративные системы. Для них характерно использование множества компьютеров, архитектура клиент-сервер, специализация сер-

веров, наличие единого информационного пространства, разветвленная сеть приема-передачи данных. Базы данных КИС содержат огромные объемы данных и обладают всеми признаками сложной системной организации. Информационные пространства КИС включают реляционные и объектные СУБД, транзакционные базы данных, временные ряды и числовые данные большого объема, многомерные OLAP-хранилища.

Примерами коммерческих корпоративных систем являются системы R/3 фирмы SAP, Oracle Application, Microsoft Business Solution Navision, система «Парус», прикладное решение для системы «1С: Предприятие 8.0» «Управление производственным предприятием», корпоративные информационные системы фирмы «Атлас», корпоративные информационные проекты на базе технологии Lotus Notes/Domino. В [2] рассмотрены гибридные интеллектуальные системы, которые позволяют эффективно соединять формализуемые и неформализуемые знания за счет интеграции традиционных средств искусственного интеллекта, примеры слияния корпоративных и интеллектуальных систем.

Дополним сделанный ранее обзор информацией об использовании ИАД в коммерческих корпоративных системах.

Комплексным программным решением сферы бизнес-аналитики, обеспечивающим быстрый доступ к информации и использование ее в принятии стратегически важных решений фирмы SAP, является подсистема SAP Business Intelligence (SAP BI). Основой решения является хранилище данных, разработанное для хранения внутренней и внешней информации, включающей документацию, видео- и аудиоклипы. Оно объединяет информацию по всей платформе SAP Business Suite и предоставляет возможность быстро реагировать на изменения рынка, контролировать показатели основных факторов успеха, анализировать и оптимизировать производительность предприятия на основе единой бизнес-модели.

Компания Oracle предоставляет полный спектр продуктов в области интеллектуального анализа данных – от различных инструментальных средств до готовых приложений – и предлагает их использование в соответствии с проблемами пользователя. Наиболее популярными инструментами являются Oracle OLAP и Oracle Data Mining. Средства OLAP (оперативная аналитическая обработка данных) полезны там, где речь идет о многомерных показателях, их иерархическом агрегировании и детализации, моделировании.

Microsoft SQL Server 2008 предоставляет интегрированную среду для создания моделей интеллектуального анализа данных и работы с ними. Эта среда называется Microsoft SQL Server Analysis Services и состоит из набора специальных инструментов (Business Intelligence Development Studio, SQL Server Management Studio, Microsoft SQL Server 2008 Integration Services, BI Development Studio). Данная среда включает алгоритмы интеллектуального анализа данных и средства, облегчающие разработку комплексного решения, применимого в рамках самых разных проектов.

Система «1С Предприятие 8.0» имеет специальный инструмент – «Подсистема анализа данных», которая может быть встроена в любую конфигурацию платформы. Она призвана помочь пользователям корпоративной информационной системы находить ответы на нетривиальные вопросы. Обеспечивает автоматизированное преобразование данных, накопленных в корпоративной информационной системе, в практически полезные и хорошо интерпретируемые закономерности, реализует группировку относительно сходных объектов; поиск устойчивых комбинаций событий и объектов (ассоциации); обеспечивает построение причинно-следственной иерархии условий, приводящей к определенным решениям (дерево решений).

Особенностью многих коммерческих корпоративных систем является то, что системы безопасности изначально в их состав не входят, а, несмотря на наличие инструментария, должны подбираться и приобретаться отдельно.

Это приводит к дополнительным затратам (финансовым, временным, трудовым, материальным и т.д.) при приобретении, настройке и эксплуатации систем, требует разработки согласований при интеграции двух разнородных систем.

Интеллектуальный анализ данных в обеспечении информационной безопасности

Современные компьютерные системы и сети находятся в состоянии постоянного развития и модификации, а объемы анализируемых данных в мире удваиваются каждый год. Поэтому для обеспечения требуемого уровня защиты информации необходимо гибко и оперативно реагировать на изменяющиеся условия, обеспечивать надежную защиту с учетом постоянного изменения входных воздействий, предупреждать действия злоумышленников, т.е. иметь адаптивную и саморазвивающуюся СЗИ.

Целью данной работы является разработка методики применения интеллектуального анализа данных для построения адаптивной саморазвивающейся системы защиты информации в корпоративных системах.

Необходимость использования инструментария интеллектуального анализа данных в СЗИ корпоративных систем проистекает из разнородности структур информационных пространств этих систем; сложности получения аналитической информации из баз данных значительного объема; большого числа пользователей, одновременно работающих в системе; требований постоянного контроля функционирования и принятия обоснованных управленческих решений, зависящих от множества факторов.

Предпосылками использования ИАД в КИС является клиент-серверная технология, распределенные базы данных, наличие хранилищ информации, применение современных сетевых технологий и разнообразного инструментария, используемого для сбора, обработки, визуализации и анализа данных.

Особенностью систем защиты информации в корпоративных системах является комбинация как минимум трех проблем: защита информации в компьютерных сетях; обеспечение безопасности баз данных; обеспечение безопасной работы систем автоматической обработки информации [3].

К часто используемым в компьютерных сетях интеллектуальным средствам относят базы знаний в составе экспертных систем, системы на основе байесовского метода, нечеткие логические системы, нейронные сети, эволюционные методы и гибридные интеллектуальные системы. Основными задачами, решаемыми интеллектуальными средствами обеспечения информационной безопасности компьютерной сети, являются классификация и кластеризация.

С интеллектуальными средствами обеспечения безопасности БД можно познакомиться в [4]. Указано, что система информационной безопасности баз данных должна использовать средства и объекты применяемой системы управления базами данных (СУБД), объекты и средства базы данных, набор правил и событий, характеризующих действия пользователей. В [5] указано, что именно фиксация событий позволяет составить представление о том, чем интересуется каждый из пользователей, составлен перечень основных регистрируемых событий.

К средствам обеспечения безопасной работы систем обработки информации относятся механизмы предотвращения вторжений, авторизация, разграничение прав доступа, криптозащита (на носителях информации, в сетях, парольная защита), управление полно-

мочиями пользователей. С целью контроля состояния системы используют базы сигнатур известных атак, а в качестве основных источников информации – системные журналы и файлы, анализируют содержимое сетевого трафика и файлов.

При традиционном подходе к построению системы защиты с применением инструментария ИАД используются искусственные нейронные сети, деревья решений и алгоритмы классификации, методы нечеткой кластеризации, ассоциативные правила, алгоритмы ограниченного перебора, кластерный анализ.

Нейронные сети используются для контроля трафика защищаемой локальной сети, поиска скрытых закономерностей в массивах первичных данных, выявления вторжений. Для предсказания значения целевого показателя используются наборы входных переменных, математических функций активации и весовых коэффициентов входных параметров. Выполняется итеративный обучающий цикл, нейронная сеть модифицирует весовые коэффициенты до тех пор, пока предсказываемый выходной параметр соответствует действительному значению. После обучения нейронная сеть становится моделью, которая применяется при прогнозировании.

Механизмы классификации используются на первоначальном уровне, например, для систематизации способов защиты (нечеткие заключения) по вектору нечетких признаков угроз. Если достоверность классификации по известным угрозам меньше некоторого уровня, то при наличии признаков атаки классификация расширяется за счет введения новой градации в классификацию – решается задача кластеризации угроз. Ассоциации выявляют причинно-следственные связи и определяют вероятности или коэффициенты достоверности, позволяя делать соответствующие выводы.

В основном публикации о применении интеллектуальных систем защиты информации посвящены системам обнаружения атак, основанных на модели, предложенной Деннингом. Модель содержит набор профилей для легальных пользователей, сравнивает текущие действия с соответствующим профилем, обновляет профиль и сообщает о любых обнаруженных аномалиях.

Недостатками традиционного подхода являются:

1. Базы знаний формируются экспертами, т.е. принцип включения в них ситуаций субъективен.

2. Базы знаний необходимо периодически обновлять, упорядочивать, систематизировать, что является трудоемкой и дорогостоящей процедурой.

3. При традиционном подходе существует задержка во времени между появлением новой атаки и средств защиты от нее (запаздывающее противодействие).

4. Атаки постоянно видоизменяются, совершенствуются, «маскируются» под стандартные процедуры, что требует постоянного совершенствования, усложнения средств защиты.

С учетом вышесказанного проблема эволюционного развития систем информационной безопасности (СИБ) актуальна.

Построение адаптивной саморазвивающейся системы защиты

Построение модели интеллектуального анализа данных является частью масштабного процесса, в который входят все задачи, от формулировки вопросов выбора и хранения данных и создания модели до развертывания модели в рабочей среде. Перейдем к описанию особенностей построения адаптивной саморазвивающейся системы.

В табл. 1 приведен перечень основных источников данных и содержащаяся в них информация, подлежащая анализу.

Таблица 1 – Источники анализируемых данных

Источник данных	Анализируемая информация
log-файлы работающих подсистем	время и тип выполняемых операций, сущность операций, соответствие пароля, сбои при установке связи с удаленной машиной, диагностика аварийных остановов
сетевые трафики	загрузка сетевого оборудования, использование каналов связи, сетевая активность
справочники и журналы регистрации пользователей и событий	ID-коды пользователей, корректность паролей, выполняемые действия
перечни функциональных задач	цепочки взаимосвязанных вызовов задач и процессов
информация о правах доступа	соблюдение регламента обращений к ресурсам
сведения о работе почтовой системы	статистика, объемы и адресность рассылок и почтовых поступлений, тематика сообщений
текстовые файлы	тематическая направленность
книги Excel	безопасность, наличие/отсутствие макросов
таблицы с атрибутами исполняемых файлов	типы файлов, даты создания и изменения, авторы изменений и их права, контроль «неизменности», адреса эталонных модулей, контрольные суммы

Источниками данных для анализа являются системные журналы событий, временные файлы серверов и рабочих станций, log-файлы работающих подсистем, сетевые трафики, справочники и журналы регистрации пользователей и событий, перечни функциональных задач и информация о правах доступа, сведения о работе почтовой системы, текстовые файлы, книги Excel, электронные сообщения, таблицы с атрибутами исполняемых файлов и т.д.

Рабочие гипотезы:

1. Активность пользователей, целевые обращения к ресурсам системы и происходящие в системе процессы можно зафиксировать и построить их адекватную модель.
2. Событие (или последовательность событий), соответствующее обобщенной модели атаки, действительно является атакой, и применение алгоритмов опережающего или одновременного противодействия является обоснованным.
3. Система может отследить работу программного обеспечения системы и, обнаружив его повреждение, восстановить защиту, выполнить автоматическую докачку потерянных или поврежденных файлов.

Механизм применения ИАД для адаптивной саморазвивающейся СЗИ можно разбить на ряд этапов.

1. Постановка задачи. На этом этапе выполняется анализ требований, определяются проблемы, которые будут решаться, метрики, по которым выполняется оценка модели, а также определяются задачи для проекта интеллектуального анализа данных. На этом этапе исследуются уровни конфиденциальности данных, потребности и права пользователей в отношении доступных данных, методы идентификации и аутентификации, традиционно используемые на предприятии.

При этом риски информационной безопасности системы могут быть определены как функция трех переменных:

– вероятности существования угроз (потенциально возможных событий, преднамеренных или случайных, которые могут оказать нежелательное воздействие на корпоративную систему или её части, либо на информационные активы и, как следствие, на бизнес-процессы компании);

– вероятности существования уязвимостей (недостатков или недоработок в системе, из-за которых становится возможным нежелательное воздействие на нее со стороны злоумышленников, неквалифицированного персонала или вредоносного кода);

– потенциальных убытков, которыми являются потенциально возможные прямые и косвенные финансовые потери, полученные вследствие реализации угроз и наличия уязвимостей.

Наиболее актуальными угрозами информационной и сетевой безопасности корпоративных систем являются:

– угрозы, связанные со злонамеренной модификацией параметров функционирования системы внутренними нарушителями или неквалифицированными пользователями;

– угрозы несанкционированного доступа к конфиденциальной информации, имеющейся в системе и сети корпорации, с целью ознакомления, модификации или блокирования;

– угрозы, связанные с разграничением прав доступа и сложностью администрирования в распределенной системе;

– угрозы, связанные с вирусной атакой на рабочую станцию пользователя, локальную или корпоративную сеть предприятия;

– угрозы, связанные с передачей информации по каналам связи и работе в сети Internet (возможное деструктивное действие различных вредоносных программ), потенциальная угроза безопасности как с точки зрения несанкционированного доступа к информации извне, так и просто из-за возможности несанкционированной работы пользователей в Интернете.

2. Сортировка и очистка данных. На этом этапе данные упорядочиваются, удаляются недопустимые и ошибочные комбинации, определяются первоисточники данных, строятся согласования, подбираются, например, столбцы, данные из которых могут быть использованы в анализе. Данные могут находиться в разных подразделениях компании и храниться в различных форматах, что потребует применения механизмов интеграции гетерогенных систем.

Алгоритмы сортировки оцениваются по скорости выполнения и эффективности использования памяти. Если алгоритм сортировки использует только абстрактную операцию сравнения ключей, то его вычислительная сложность $O(n\log n)$ операций сравнения. При параллельном вычислении n ситуаций можно отсортировать за $O(\log^2 n)$ операций, а худшими являются алгоритмы сортировки, вычислительная сложность которых – $O(n^2)$ операций. Требуемый объем памяти для реализации алгоритмов сортировки, как правило, составляет $O(\log n)$ ячеек.

Методы сортировки, рекомендуемые для использования в системе: сортировка вставками (может сортировать список по мере его получения), блочная сортировка (относится к классу быстрых алгоритмов с линейным временем исполнения O(N)).

3. Классификация регистрируемых событий, например, угроз по вектору признаков атак и механизмов защиты по вектору угроз, выделение кластеров. Используются средства, упрощающие разделение данных на набор данных для обучения и проверочный набор данных.

Задача классификации – одна из наиболее распространенных задач в анализе данных. На сегодняшний день разработано большое число подходов к решению задач классификации, использующих такие алгоритмы, как: деревья решений, нейронные сети, логистическая регрессия, метод опорных векторов, дискриминантный анализ, ассоциативные правила. Одним из эффективных алгоритмов классификации является так называемый «наивный» (упрощенный) алгоритм Байеса. С точки зрения быстроты обучения, стабильности на различных данных и простоты реализации, алгоритм Байеса превосходит практически все известные эффективные алгоритмы классификации. Обучение алгоритма

производится путем определения относительных частот значений всех атрибутов входных данных при фиксированных значениях атрибутов класса. Классификация осуществляется путем применения правила Байеса для вычисления условной вероятности каждого класса для вектора входных атрибутов. Входной вектор приписывается классу, условная вероятность которого при данном значении входных атрибутов максимальна. Алгоритм строится в предположении, что входные атрибуты условно (для каждого значения класса) независимы друг от друга [6].

4. Предварительный статистический анализ данных, получение контрольных метрик и закономерностей. Создание структуры интеллектуального анализа данных. В дальнейшем эти данные могут использоваться несколькими подсистемами интеллектуального анализа, например, уже упоминаемыми ранее подсистемами нерегламентированных действий пользователей или системой анализа вторжений, модели которых построены по одной структуре.

5. В дальнейшем результаты предыдущих пунктов представляются в виде систем нечетких правил, которые реализуются в виде специализированных структур, подбор классификаторов, формирование признака структуры (Ps). Анализ данных и формирование признаков происходит постоянно и независимо от дальнейшей работы алгоритма. Изменение параметра Ps свидетельствует об изменении условий внешней среды (появление, например, нового вида атаки и необходимости либо выбора иной модели процесса, либо обучения прежней на новом наборе данных).

Правила представляются в виде «если» – «то» и также используются для прогнозирования. На основе частоты встречаемости логических закономерностей делается вывод о возможном событии. Например, цепочка MD – COPYA3 – ARH – WWW – DEL – ассоциируется с копированием информации из конфиденциального источника и передачей его по Internet-каналам.

6. Построение модели. На этом этапе модель представляет собой просто математическое выражение, контейнер, еще не наполненный данными. При этом, если возникает необходимость изменения данных, это приводит к необходимости обновить и структуру, и модель интеллектуального анализа данных, изменить признак Ps.

Перед развертыванием модели в рабочей среде необходимо проверить эффективность работы модели. Кроме того, во время построения модели обычно создается несколько моделей с различной конфигурацией, а затем проверяются все модели, чтобы определить, какая из них обеспечивает лучшие результаты для поставленной задачи и имеющихся данных.

7. Передача опыта адаптивной СЗИ (наследование) по обеспечению информационной безопасности.

8. Обучение классификаторов на обучающей выборке подмножеству входных векторов, формирование информационных полей четких классификаторов.

9. Адаптация системы к реальным условиям.

10. Коррекция матриц экспертных оценок и систем нечетких правил по результатам адаптации.

При этом решение о расширении классификаций атак и механизмов защиты производится в соответствии с системой оценок достоверности нейтрализации угроз в разрезе отдельных механизмов защиты. Обосновать целесообразность использования механизма защиты в составе многоуровневой СЗИ можно, например, по матрице достоверности использования механизмов защиты для нейтрализации угроз [6]:

$$x_i = \sqrt[n]{\prod_{j=1}^{n} me_{ij}}, \qquad i = 1, ..., m ,$$

где me_{ij} – элементы матрицы достоверности «угрозы – механизмы защиты».

11. Формулирование новых нечетких правил в случае расширения классификации.
12. Формирование комплекса оценок защищенности системы.
13. Анализ структуры классификаторов и выявление недостатков в системе защиты, включение в систему дополнительных механизмов защиты, контроль целостности данных и программных модулей.
14. При необходимости – восстановление программной среды, изменение структуры системы информационной безопасности.

Использование эффективных алгоритмов

Одной из наиболее важных задач при обеспечении безопасности компьютерной системы является сбалансированность уровня её защищенности и производительности. Применение средств защиты информации в корпоративной системе снижает ее производительность по обработке пользовательской информации ввиду дополнительных затрат времени на реализацию функций защиты. Уровень защищенности и производительность компьютерной системы находятся в обратно пропорциональной зависимости друг от друга, т.е. с ростом уровня защищенности снижается производительность и наоборот.

Но построение адаптивных саморазвивающихся систем защиты невозможно без быстродействующих алгоритмов. Например, как было указано выше, одним из недостатков традиционного подхода является задержка во времени между появлением новой атаки и средств защиты от нее.

В теории СЗИ различают одновременное, опережающее и запаздывающее противодействие. Запаздывающее противодействие – когда реакция системы защиты начинается к моменту завершения угрозы или после нее. Одновременное противодействие – то, что начинается с появлением угрозы. И, наконец, противодействие, носящее опережающий характер, – когда реакция системы защиты начинается до начала реализации угрозы.

Идеальным вариантом является опережающее противодействие, а для этого необходимо не только наличие методик, позволяющих своевременно обнаружить угрозу безопасности системе, но и применение алгоритмов, способных выполнить анализ ситуации и выявить предпосылки для такого вторжения. Применение Т-эффективных алгоритмов [7] при решении задач сортировки, дешифрации, распознавания и их использование в системе защиты позволяет добиться не только одновременного, но в ряде случаев и опережающего противодействия.

В заключение укажем ряд направлений в корпоративной системе водоснабжающей отрасли, где также необходимо применение ИАД.

1. Биллинговые подсистемы. Методы и средства интеллектуального анализа данных необходимы для контроля данных по абонентам, выявления сложных взаимосвязей типа параметра «недействующий лицевой счет», в формирование которого включено до 18 начальных признаков.

2. Системы контроля отгрузки продукции («водомерный учет»). При этом исходной рабочей структурой являются водопроводные и водоотводящие сети предприятия. Механизмы ИАД необходимы для выявления наиболее вероятных мест хищения продукции (незаконные врезки).

3. Системы прогноза получения оплат за отгруженную продукцию («недобросовестный потребитель»). В этих подсистемах производится анализ финансовых рисков, связанных с фактическим кредитованием потребителей, что возникает по причине работы отрасли по схеме: первое событие – отгрузка, последующее – оплата.

Среди особенностей описываемой СЗИ хотелось бы подчеркнуть следующее:

1. Одной из функций системы является анализ «неповрежденности» вирусными атаками программных модулей корпоративной системы, для чего строятся, при замене версий программных продуктов корректируются, а в процессе работы системы постоянно контролируются матрицы атрибутов программных файлов (MaPF).

2. Самовосстановление системы выполняется автоматически при получении от системы ИАД сигнала о несоответствии исходной (эталонной) и текущей MaPF. Кроме того, по регламенту или команде системы анализа происходит и запуск процедуры восстановления данных (Backup-Restore).

3. Система «не зависит» от своих частей. Каждая часть может функционировать и восстанавливаться отдельно и независимо.

Кроме того, ИАД необходим для анализа и фильтрации электронной почты масштаба предприятия, классификации Web-операций, рубрикации электронных документов организации, анализа корпоративных учетных данных, финансово-экономических зависимостей.

Выводы

Интеллектуальный анализ данных является необходимым и современным дополнением такой крупной информационной структуры, как корпоративная система. Одной из её составных частей является система защиты информации. Средства защиты должны постоянно совершенствоваться и развиваться, ввиду чего предложенный в работе механизм построения адаптивной саморазвивающейся СЗИ является актуальным, а использование наряду с ИАД быстрых алгоритмов увеличит эффективность системы, что является темой отдельного исследования.

Литература

1. Han J. Data Mining: Concepts and Techniques / J. Han, M. Kamber // Morgan Kaufmann. – 2000.
2. Маслова Н.А. Концептуальные особенности построения интеллектуальных корпоративных систем предприятий водоснабжающей отрясли / Н.А. Маслова // Штучний інтелект. – 2006. – № 4. – С. 443-452.
3. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – Изд-во: ДМК, 2002. – 134 с.
4. Корнеев В.В. Базы данных: интеллектуальная обработка информации / В.В. Корнеев, А.Ф. Гареев, С.В. Васютин, В.В. Райх. – М. : Нолидж, 2000. – 352 с.
5. Маслова Н.А. Информационная безопасность систем управления базами данных / Маслова Н.А. // Комп'ютерна математика. Оптимізація обчислень : зб. наук. праць. – Київ : ІК НАН України, 2001. – Т. 1. – С. 271-280.
6. Гончаров М. Модифицированный древовидный алгоритм Байеса для решения задач классификации / Гончаров М. – Spellabs, 2007.
7. Задірака В.К. Т-ефективні алгоритми наближеного розв'язування задач обчислювальної математики / В.К. Задірака, М.Д. Бабич, А.І. Березовський та ін. – К., 2003. – 216 с.

Н.А. Маслова
Про застосування інтелектуального аналізу даних з метою захисту інформації у корпоративних системах
У статті пропонується методика побудови адаптивної системи захисту для корпоративних систем, що має змогу розвиватися самостійно. При побудові системи використано методи і базові прийоми інтелектуального аналізу даних. Система призначена для рішення єдиної задачі захисту комп'ютерних мереж, баз даних і систем автоматичної обробки інформації. Наведено елементи використання методології інтелектуального аналізу даних у системі водопостачальної галузі.

N.A. Maslova
About Application of Intellectual Data Mining for Security of the Corporate Systems
The method of construction of adaptive systems of security for the corporate systems is offered in the article. For construction of the system are used methods and base approaches of intellectual data mining. System is intended for the decision of single task of defence of computers networks; databases and systems of automatic processing of information. The elements of the use of methodology of intellectual data mining in the system of water-supply industry are offered.

Статья поступила в редакцию 02.06.2009.